

From: Trout, Dennis (MIL)
Sent: Friday, August 20, 2010 2:50 PM
To: MIL DL ALL STATE STAFF
Subject: Replacement of File Server
Importance: High

As many of us have noticed, we have been experiencing sporadic issues with access to large individual PST and data files (usually Access database or Excel spreadsheets) that are currently being stored on the file server (MILFLCPM01). This problem has been traced to a hard drive failure that impacts the server operating system not the data storage hard drives. This failure in turn impacts access to the larger files as it interprets the hard drive failure as a lack of operating system memory available to open or move the larger files.

We have just completed an internal reallocation of hardware so we now are able to begin the migration of your personal and organizational shared folders over to the new server hardware. One of the things we will also be accomplishing during this migration is a file restructuring so that we can create rules that will automatically map your personal folder every time you logon to the a computer. This mapping will happen regardless of which computer system you logon to on the MIL.WA.GOV network. The only drive mapping required by IT support or you individually will be those folders you share with other staff or organizations please rest assured, all your folder security permissions will be retained.

Starting next Wednesday afternoon, August 25th, we will begin working with individual sections to migrate folders over to the new system. Because of the complexity of the migration, our intent is to move staff by organizational section vice the entire server at once. This way, we can double check that all data has successfully been migrated and access and automatic mapping is working properly. We will contact individual organization sections and arrange the migrations in advance. This will give us the opportunity to answer any questions and concentrate on a particular section's requirements as we make the changes.

There is one area that each of you can assist us with to ensure success of this migration. Please review your personal files stored on the file server prior to August 25th and remove any non-work related items such as personal photos & movies (i.e.: family reunions, birthday or wedding parties), music MP3 files, etc. Files of this type consume large amounts of hard drive space that we cannot afford to allocate on our servers to store. If you have these types of files or folders on the system, please copy them off so you can take them home and lastly please delete them from your folders.

If you have any questions, please do not hesitate to ask as we will strive to provide you a prompt answer. Your questions and feedback are important as you may have a special folder or database that we are unaware of which needs special handling and consideration. We want to make sure we capture all the mission critical data in order to make this migration as complete as possible.

Thank you for your assistance in making this migration as smooth as possible and your patience & understanding as we repair a failing system as we continue to support you our customers.

Tim

From: Trout, Dennis (MIL) [Dennis.Trout@mil.wa.gov]
Sent: Thursday, October 07, 2010 12:31 PM
To: Masculino, Jocelyn (MIL); Fraga, Vicki; Toft, Edward (MIL)
Subject: Movement of Files to the New File Server

We can go ahead and begin moving individual folders over to the new file server storage MILNACPM03. The "USERS" and "SHARED" folders are already created for use. We do not necessarily need to change the name of the server to MILFL something as to the user, it will not matter since the only thing they care about is the Drive Letter they are mapped to.

If you move an individual's or shared folder over, only move the mission items. Any personal photos, movies, Barbie Pole Dancing clips, etc. will not get moved.

I talked with Tom and he wants us to expend the time and effort moving only the mission files vice scanning and deleting the non-mission files and then moving the remaining files over. the non-mission files will remain on the old File Servers for two weeks and then the servers will be decommissioned and the non-mission correspondence destroyed. If the owner does not get it copied out to dvd/cd/thumb drive, then it is their problem.

We are going to need to coordinate the migration of the folders most likely by section as they will need to access the shared folders to accomplish any work. I am confident this is something we can accomplish ourselves without requesting a PLAN.

Let me know your thoughts/ideas and we can move forward now.

Thanks.

Dennis M. Trout
IT Operations Branch Manager
Washington State Military Department IT Division
IT Operations Branch
(253) 512-7391
e-mail: dennis.trout@mil.wa.gov

Tom,

With your approval, I will schedule Vicki and Ed to complete an updated scan/review of the File Server and individual computers systems this afternoon for EMD. Based upon comments and past experiences and observed practices, we are sure that individuals are simply moving their inappropriate files and folders from the File Server over to their individual workstation awaiting the completion of the migration to the new file storage system at which time they will simply recopy the files and folders over to the new file storage system.

I intend to validate that either they are completely removing the materials from State owned computer systems or that they are playing a *Shell Game* as already observed. This is something that must be accomplished and corrected or we will simply be refilling the new system with JUNK.

We will be completing the revalidation in an unobtrusive manner using System Center. We will not be interfering with the customers operations.

Thanks for your support.

Dennis M. Trout
IT Operations Branch Manager
Washington State Military Department IT Division
IT Operations Branch
(253) 512-7391
e-mail: dennis.trout@mil.wa.gov

From: Toft, Edward (MIL)
To: Trout, Dennis (MIL)
Cc: Fraga, Vicki (for Trf to WA); Masculino, Jocelyn (MIL)
Subject: re: milwkeoc48 (right side)
Date: Tuesday, January 18, 2011 2:09:06 PM

Dennis,

Milwkeoc48 has been re-imaged. I have told the duty officers to log on and see if there is anything missing and to notify IT (via helpdesk@emd.wa.gov). This should stop any further pornographic pop-ups on that machine (at least until they use it). Also, I deleted their shortcut to www.live365.com as well as other streaming music/movie stations (lets see if they report them as missing).

We really need to lock down the machines (all of them on the network) to reduce the frivolous overhead this causes on staff.

Again, please talk to Mr. Muehleisen, the CISO or HRO to see what we can actually do, if we can get any support to follow the computer use policy and any enforcement of it.

Re: You tube videos, personal pictures, pornographic pictures, users music (CD and iTunes collections), gun manuals, shortcuts to weapon websites, etc, stored on users computers, saved on the file servers and backed up.

Thank you,

Edward L. Toft II, BSIT
IT Network Administrator & Desktop Operations Specialist
Washington State Military Department, IT Division
IT Operations Branch
Network & Desktop Operations Section
Desk: (253) 512-7439
Blackberry: (253)468-1680
e-mail: edward.toft@mil.wa.gov

The audit of servers (milflcpm01, milflcpm001) were not complete and does not show the exchange server (milmxcpm2003a) which shows how much users use the exchange server for personal email. There are other servers which need to be audited. The audit of the workstation only shows what the user has saved on their computers not browsing history. Many users are on Facebook most of the day, play Farmville, watch Mariners and Seahawk games, stream music and surf YouTube. Some IT staff has made videos of users playing Farmville and also taken pictures of users violating the IT/ Network policy and reported this to Dennis Trout. Mr. Trout states, "It is up to their supervisors to handle, not us". The audit of EMD (not MIL) workstations is partial and does not include external hard drives, thumb drives and other storage media (CD/DVD, zip) which users use regularly. The use of state asset external storage devices has been found to contain a mix of personal information (pictures, music, childrens stuff, etc.) as well as work related items and documents. Many users state they use these(issued and personal drives) to move information between their personal computers at home and work computers. This practice is allowed and endorsed by unit supervisors and management. IT management (Dennis Trout) has been made aware of this through email (for written documentation), and verbally from IT staff.

Many staff have workstations as well as laptops and/or 'flyaway' kits. I believe there are almost 2 computers per employee at EMD. If it was not physically plugged into the network during the audit, it did not get counted. Many employees have resorted to using their laptops for home use. An audit of ALL laptops and flyaway kits as well as aircard usage would verify this in black and white.

Even the "Use of the Internet, Electronic Mail, Computer System Policy 05-004-05" policy itself was defaced years ago by a former employee and is still to this day. People find this a joke and say it just shows how much emphasis the MIL Department really puts on IT and the policy.



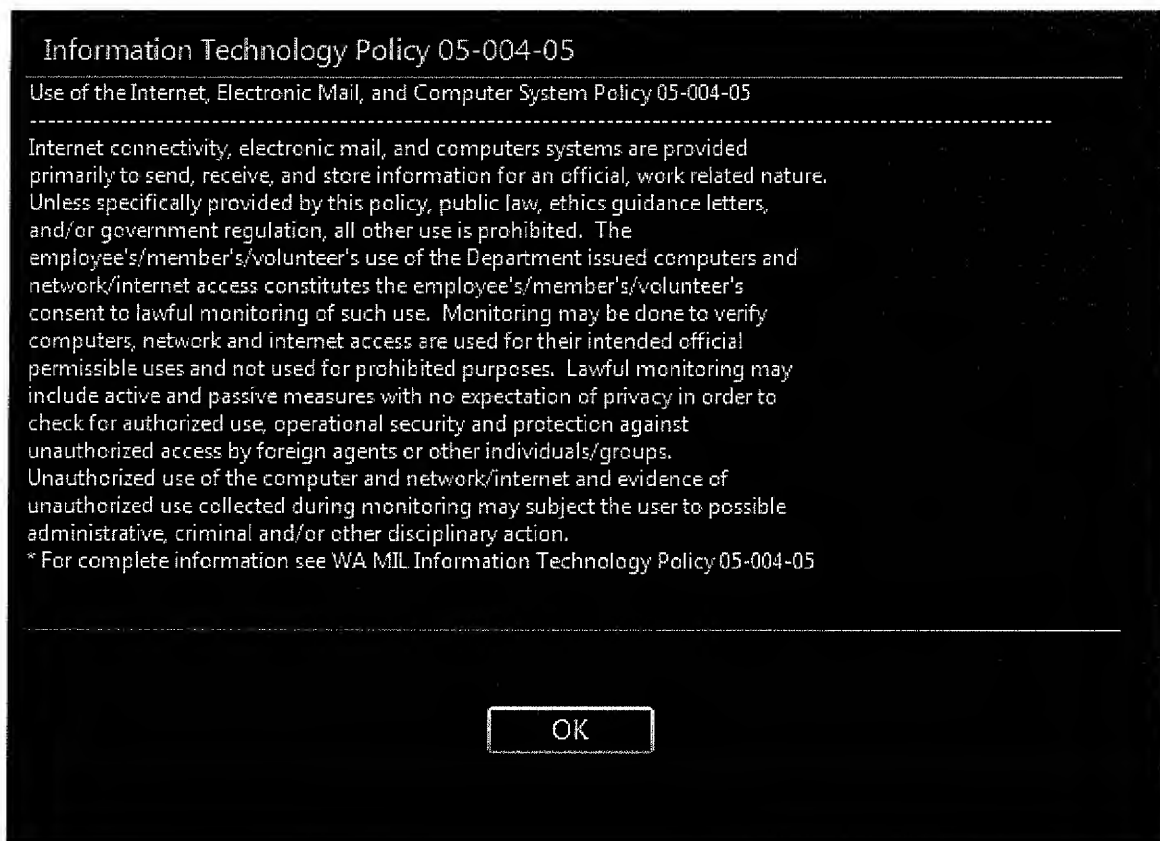
WASHINGTON MILITARY DEPARTMENT POLICY

Information Technology Policy 05-004-05

**USE OF THE INTERNET, ELECTRONIC
MAIL AND COMPUTER SYSTEMS**

Supersedes Administrative Policy 00-004-04 dated January 2004

Users see a Computer use agreement which they must click 'ok' on before they can log onto their computers. This is taken directly from the "Use of the Internet, Electronic Mail, Computer System Policy 05-004-05". This has been in place for over 1 year. Users still violate this policy because there is no enforcement of it.



IT staff are tired of reporting violations to IT management and nothing happening. Users have found that they do not have privileges to install software, so they have learned to go around it. They install the software at home on a USB device (thumb drive, external HDD) and come to work and plug it in. IT staff have confiscated one of these and turned it into Mr. Trout. Staff was told to return it as it was personal property (the user continues this practice). Users have introduced virus' into the MIL network by doing this (document in the helpdesk, verbally by users and in email). When IT staff show up at a users desk to assist with the resolution of a trouble ticket submitted by the user, IT staff sometimes must wait for the user to close the streaming music, save their game, or log off an online chat session. Sometimes users simply ask IT staff to come back after their soap opera, tv show, or at halftime in the game they are watching online. Some users have mapped their Outlook (email) and their personal email. So their personal email is delivered to the work outlook client. Also, users use their work email as the personal email. This has been documented in screenshots, videos and pictures.

Employees regularly sell apples, pigs, girl scout cookies, etc. at work. They print the flyers from their computers at work and post around the agency and in the EMD break room. Any employee that

works at the agency is aware of this and has probably received emails about it. IT has taken pictures and sent emails to Dennis Trout about this.

Users have been observed and reported for using state commercial CD/DVD burning equipment to pirate and make illegal copies of movies (rented and owned by users) as well as software.

****A full audit of ALL servers and workstations needs to be performed to honestly show the true extent of the misuse and abuse of state resources happening in the Washington Military Department.**

From: Toft, Edward (MIL)
Sent: Friday, February 04, 2011 2:59 PM
To: Trout, Dennis (MIL); Masculino, Jocelyn (MIL); Fraga, Vicki (for Trf to WA)
Subject: Info on new Group Policy....

All,

Now that you all know anyway via word of mouth, here is the formal written documentation of the new group policy: In an effort to help combat the blatant disregard of the MIL IT Policies by 90%+ of EMD staff, On 2/3/11 (afternoon) I have added the IE Delete policy to EMD DIRS, EMD E911, EMD EOC, EMD MRR and EMD PET. This new group policy prevents users from deleting their browsing history, temp internet files and cookies, or using IE InPrivate web browsing. Below is a screenshot for documentation.

I only applied this to EMD as I do not feel comfortable applying it outside of EMD on the MIL without proper consultation and support of "management".

The screenshot displays the Group Policy Management console. On the left, the tree view shows the hierarchy: Group Policy Management > Forest: wa.lc > Domains > mil.wa.lc > Domain Users > EMD DIRS > IE Delete. The right pane shows the configuration for the 'IE Delete' policy. It includes tabs for Scope, Data, Settings, and Delegation. The 'Data' tab is active, showing 'Data collected on: 2/4/2011 2:50:50 PM'. Below this, 'Computer Configuration (Enabled)' is listed with 'No settings defined.' Under 'User Configuration (Enabled)', there are two sections: 'Administrative Template' and 'Windows Components/Internet Explorer/Delete Browsing History'. The 'Delete Browsing History' section has a 'Policy' that states: 'Prevent Deleting Web sites that the User has Visited', 'Prevent the deletion of temporary Internet files and cookies', and 'Turn off "Delete Browsing History" functionality'. The 'Windows Components/Internet Explorer/InPrivate' section also has a 'Policy' that states: 'Turn off InPrivate Browsing'.

*SUA SPONTE!

[REDACTED]

From: Toft, Edward (MIL)
Sent: Tuesday, February 15, 2011 8:25 AM
To: Fraga, Vicki; Masculino, Jocelyn (MIL); Toft, Edward (MIL); Trout, Dennis (MIL)
Cc: Glenn, Mark E. (MIL)
Subject: Deleting history, cookies, etc...

All,

We need to address the issue of when (scheduled or not), how (do we also document and report signs of misuse and abuse per policy), who (who does it, is there a witness).

*This email is being generated in response to work order 18069, and the server and workstation audit findings recently given to Dennis. I look forward to a "team" discussion and quick resolution of the many IT policy violations and RCWs being violated.

Mark, including you as the former IT network supervisor and new CISO/Plans Manager.

Edward L. Toft II, BSIT
IT Network Administrator & Desktop Operations Specialist
Washington State Military Department, IT Division
IT Operations Branch
Network & Desktop Operations Section
Desk: (253) 512-7439
e-mail: edward.toft@mil.wa.gov

><(((0>...><(((0>
><(((0>...><(((0>

From: Trout, Dennis (MIL)
Sent: Thursday, February 17, 2011 5:43 PM
To: Toft, Edward (MIL)
Cc: Masculino, Jocelyn (MIL); Fraga, Vicki
Subject: Request for Supporting Documents

Importance: High
Sensitivity: Confidential

Ed,

I have read your comments provided to me after today's Section Meeting and I appreciated your continued efforts to identify those outside the acceptable parameters of IT resource usage. I have a meeting with our CIO, Major Thomas Muehleisen, tomorrow, at 10AM.

I need you to provide me any and all documentation (printed material, photos, videos, etc.,) which was not included in the audit material and that you have made of Improper Use of State Equipment by Military Department employees so I may provide it to our CIO at tomorrow's meeting. Without this evidence/documentation, I will only be providing hearsay of which I am fairly confident management will require tangible documentation before proceeding further.

As you are well aware, as I have shared the comments made to me when I report abuses to the responsible supervisors, I have and continue to work towards management involvement and action regarding this massive problem. You are correct that without management's support this problem will never be resolved and that is why I continue to approach my supervisor and those supervisors responsible for violators. But as you appropriately commented in your document, "it is up to the supervisor to handle". As I have pointed out many times, the Military Department Policy 05-004-05 is specific in that the "First line Supervisor require employee compliance, report misuse and take recommended appropriate corrective or disciplinary action." Once I have reported it to the first line supervisor and my supervisor, the ball is literally out of my court or hands.

This has not however prevented me from continuing efforts to have you, Jocelyn and Vicki continue to identify those individuals abusing the acceptable use of our equipment and its intended use by the Department.

I appreciate your frustration as I share it. I will push forward the results from the recent audit, which I requested authorization for from my supervisor, and hopefully something will begin rolling through our collective continued efforts.

I hope it is acceptable that I included Jocelyn & Vicki on this email as I need and want them to provide me any documentation of misuse as well. I also recalled that Vicki read or browsed your memo this morning prior to my receiving it.

I will keep you and the team apprised of any results or action I become aware of regarding the presentation of this documentation to management. Please do not stop providing me with documented misuse incidents in the future.

Dennis M. Trout
IT Operations Branch Manager
Washington State Military Department IT Division
IT Operations Branch
(253) 512-7391

From: Clark, Tim (EMD)
To: Trout, Dennis (MIL)
Cc: Muehleisen, Thomas W (MIL)
Subject: FW: IT Questions (UNCLASSIFIED)
Date: Wednesday, April 27, 2011 11:13:16 AM

Dennis, as we are forced to move into a more formal approach with our staff on removing material that should not be our state systems, can you confirm for me that all EMD staff were included in the review you recently finished and provided me the results on earlier this week? Thanks.

Tim

-----Original Message-----

From: Clark, Tim (EMD)
Sent: Wednesday, April 27, 2011 11:08 AM
To: MIL DL EMD UNIT MANAGERS; MIL DL EMD SECTIONS SUPERVISORS
Cc: Mullen, Jim (EMD); Muehleisen, Thomas W (MIL)
Subject: FW: IT Questions (UNCLASSIFIED)

Folks, I have had a request to clarify some of the IT requirements on "de minimis use" of state resources in relation to our computers and phones. Please see the response from Mark Glenn below. Let me know what your questions are. I have also received the latest review of our servers. I will be providing copies to impacted unit managers and a draft verbal counseling format to utilize when counseling our staff on inappropriate use. We are now past the point where talking and asking our staff to comply is valid, without written documentation.

Tim

-----Original Message-----

From: Glenn, Mark E. (MIL)
Sent: Wednesday, April 13, 2011 8:01 AM
To: Clark, Tim (EMD)
Cc: Muehleisen, Thomas W (MIL)
Subject: RE: IT Questions (UNCLASSIFIED)

Hello Tim,

I was asked to respond to your inquiries in questions 1 and 2.

1. The Executive Ethics Board has adopted guidelines for exceptions to the no personal use standard under RCW 42.52.160(1). The Ethics Board allows limited unofficial use if:

There is little or no cost to state; (I would argue that storing non-work related pictures and photos on network resources does constitute a cost burden to the State as there are negative impacts on storage, backups and staff time accordingly.)

Any use is the most effective use of time or resources

There is no interference with the performance of official duties

The use is brief in duration and frequency

The use does not disrupt other state employees and does not obligate them to make a personal use of state resources; and

The use does not compromise the security or integrity of state information or software (I would argue that importing personal files to network resources could potentially compromise the security or integrity of state information and or software.

We fully support the "de minimis use" or common sense usage of Department individually assigned resources by the staff and the saving or storing of four to six non-offensive photos for the purpose of screen backgrounds or screen savers has always been acceptable. However, 384 Megabytes of personal family pictures, wedding videos, children's birthday parties, etc., does not constitute "de minimis use" by anyone's standards. The storing of over 500 Megabytes of music, pictures of questionable material or

subject matter and the drawings and photos covering the complete remodeling of one's home on an individual's local hard drive or on the file server do not constitute "de minimis use" of State resources.

2. Although I-Phones and I-Pads are not specifically banned at this time, current security policy does outline guidance that under no circumstances are any personally owned devices be allowed to utilize state government network resources, it is a violation of State Ethics rules. We are not instructing staff not to use their I-Phones or I-Pads however we are requesting staff that have I-Pads or I-Phones to ensure they are not utilizing state government network resources. Currently, IT staff are working to detect unauthorized access to state network resources and staff will be notified accordingly if a personally owned device is connecting to state network resources. There have been specific instances where an individual's personal I-Phone or iPad has been discovered on the State Network which is a violation of the Washington State Information Security Standards governing our network security requirements. It has been in direct response to these individual cases, in Building 20B, that IT staff have specifically notified staff that their personal devices needed to be turned off or at a minimum, the wireless communications capability must be disabled while working in Building 20B.

Please be advised I am also working to put together regular security briefings for all staff that will provide opportunities for us to provide reminders and staff to have the ability to participate in Q&A sessions. Please let me know if you need further clarification regarding these issues, thanks Tim.

Mark E. Glenn, M.S.W.
WA Military Department
Chief Information Security Officer & Plans Manager
IT Division, Building 9
Camp Murray, Washington 98430
mark.glenn@mil.wa.gov
(253) 512-8779 Office
(253) 250-1587 Mobile

-----Original Message-----

From: Muehleisen, Thomas LTC NGWA [<mailto:thomas.muehleisen@us.army.mil>]
Sent: Monday, April 04, 2011 10:21 AM
To: Clark, Tim (EMD)
Cc: Glenn, Mark E. (MIL)
Subject: RE: IT Questions (UNCLASSIFIED)
Importance: High

Classification: UNCLASSIFIED
Caveats: NONE

Will do. Please send any further questions to both Mark and myself. He'll write up responses (or consolidate from other IT staff). I think they're may be some confusion about 'de minimus'. Fed and state are different, in that regard. But, I'll craft a better response and send it to you.

-t

-----Original Message-----

From: Clark, Tim (EMD) [<mailto:T.Clark@emd.wa.gov>]
Sent: Monday, April 04, 2011 9:28 AM
To: Muehleisen, Thomas LTC NGWA
Subject: FW: IT Questions

Tom, as we continue to clean up our computers I expect we will get more questions like those below requesting clarification. We do not need an answer to #3 since you all have solved that problem and Dennis briefed it at our all staff. I would like some clarification on # 1 and 2. Thanks. I will be out on vacation from April 6-12. Can you have the results from your review of EMD's server review shortly after April 13th? Thanks.

Tim

From: Ezelle, Robert (EMD)
Sent: Friday, April 01, 2011 1:19 PM
To: Clark, Tim (EMD)
Subject: IT Questions

Tim:

In our section managers' meeting last Friday we had significant discussion about IT policy. If possible, could you approach Tom and secure clarification for us on the following issues? If you don't mind me going direct, I am perfectly happy to make the contact.

1. What are the guidelines regarding pictures on our computers and the network? IT Policy 05-004-05 does not prohibit the storing of pictures on our IT systems. The results of the network monitoring recently distributed to managers implies that nothing should be stored in the My Music, My Videos, or My Pictures folders. We fully understand the need to not overload our storage capabilities. Yet, small numbers of pictures constitute de minimis use. If we wish to have personal screen savers or wallpaper, we need to have the ability to store pictures on our computers. Can IT give us written guidance on what constitutes de minimis storage of pictures?

2. There is anecdotal information that certain IT personnel are telling people to shut down iPads and iPhones because they are pinging the network and congesting it. Again, is there a policy or guidance?

3. When I first started here, there was discussion about using thumb drives to back up data. IT promised us a policy. To date nothing has been received. Are we clear to buy/use thumb drives to store data in addition to the network backup?

Robert Ezelle

Homeland Security Section Manager

Washington State Emergency Management Division